1156.41275X00

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Applicants: Thomas MULLER et al.

Serial No.: 09/588,003

Filed: June 6, 2000

For: SECURITY ARCHITECTURE

APPEAL BRIEF

Assistant Commissioner
for Patents
Washington, D.C. 20231

December 17, 2004

Sir:

The following is an Appeal of the rejections set forth in the Office Action dated May 17, 2004 (hereinafter "Office Action").

REAL PARTY IN INTEREST

The Real Party in interest in this Appeal is Nokia Mobile Phones Limited, as evidenced by an Assignment filed on October 17, 2000 and recorded on Reel 011174 and Frame 0669.

RELATED APPEALS AND INTERFERENCES

On information and belief there are no other appeals and interference that will directly affect or be directly affected by or having any bearing on the Boards decision in the pending appeal.

STATUS OF CLAIMS

Claims 1-11, 13, 18 and 28-32 stand rejected under 35 U.S.C. §102(b) as being anticipated by U.S. Patent No. 5,163,147 (Orita). Claim 12 stands rejected under 35 U.S.C. §103(a) as being unpatentable over Orita in view of WO 99/00958 (Leveridge et al.). Claims 14-17 and 20-26 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Orita in view of BLUETOOTH: Visions, Goals, and Architecture (Haartsen et al.). Claims 19 and 27 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Orita in view of U.S. Patent No. 5,818,936 (Mashayekhi). Claims 1-32 are pending in the present application.

STATUS OF AMENDMENTS

An Amendment was filed on March 31, 2004 amending the specification and claims 3, 5, 6, 8, 16, 17, 20, 21, 27, 30 and 31 to further clarify the invention, and submitting new claim 32. A Request for Reconsideration was filed on July 19, 2004.

CONCISE SUMMARY OF INVENTION

The present invention relates to a device for communicating with other devices to allow them to access applications that includes at least a first application 118, authentication means 106 for authenticating a communicating device, and access control means 120 accessible by a communicating device requesting access to the first application without the communicating device having been authenticated by the authentication means, and arranged to arbitrate whether access of the communicating device to the first application is granted or refused. If the arbitration requires an authentication of the communicating device, the access control means

instructs the authentication means to authenticate the communicating device, (pg. 17, line 4 – pg. 18, line 24).

ISSUES PRESENTED FOR REVIEW

Whether claims 1-11, 13, 18 and 28-32 are anticipated by Orita under 35 U.S.C. §102(b). Whether claim 12 is unpatentable over Orita in view of Leveridge et al. under 35 U.S.C. §103(a). Whether claims 14-17 and 20-26 are unpatentable over Orita in view of Haartsen et al. under 35 U.S.C. §103(a). Whether claims 19 and 27 are unpatentable over Orita in view of Mashayekhi under 35 U.S.C. §103(a).

GROUPING OF CLAIMS

Each of the claims should be considered by the Board individually and separately so as not to stand or fall together.

ARGUMENTS

Appellants assert that the cited references do not disclose, suggest, or render obvious the limitations in the combination of each of pending claims 1-32 of the present application. Appellants respectfully request that all current rejections be withdrawn and the decision of the Examiner be reversed based on the following.

Rejections have been based on Orita being asserted by the Examiner under 35 U.S.C. §102(b). To anticipate a claim, a prior art reference must disclose every limitation of the claimed invention, either explicitly or inherently. *In re Schreiber*, 128 F.3d 1473, 1477, 44 U.S.P.Q.2d (BNA) 1429, 1431 (Fed. Cir. 1997). The identical

invention must be shown in as complete detail as is contained in the . . . claim. *Richardson v. Suzuki Motor Co.*, 868 F.2d 1226,1236, 9 U.S.P.Q.2d 1913, 1920 (Fed. Cir. 1989); M.P.E.P. §2131. The elements must be arranged as required by the claim. *In re Bond*, 910 F.2d 831, 15 U.S.P.Q.2d 1566 (Fed. Cir. 1990); M.P.E.P. §2131. It is respectfully submitted that the Patent Office has not met the required legal burden as set forth by the courts to substantiate valid rejections under 35 U.S.C. 102(e).

Claims 1-11, 13, 18 and 28-32 and Orita

Claims 1-11, 13, 18 and 28-32 stand rejected under 35 U.S.C. §102(b) as being anticipated by Orita. Appellants respectfully request that these rejections be reversed.

Orita discloses a computer system with file security function where environment profile information defining a file to be accessed and an executable user program are previously stored in a storage unit. The environment profile information is selected by operator profile information corresponding to ID information input via a workstation by a user. A host computer executes the user program defined by the environment profile information. When a specified file access is requested after the execution of the user program, whether execution of the file access is permitted or not is determined according to access protection information. The access protection information is information having access types and file contents defined by the environment profile information.

Regarding claims 1, 28 and 30-32, Applicants submit that Orita does not disclose or suggest the limitations in the combination of each of these claims of, inter alia, access control means accessible by a communicating device requesting access to a first application without the communicating device having been authenticated by

the authentication means, and arranged to arbitrate whether access of the communicating device to the first application is granted or refused wherein if the arbitration requires an authentication of the communicating device, the access control means instructs the authentication means to authenticate the communicating device, or arbitrating the access of a requesting device to a service provided to a providing device that includes determining, in an arbitration means, whether to grant or refuse access to a first application by the requesting device, wherein if the determination requires authentication of the requesting device, the authentication is performed during that determination and not previously, or arbitration means for determining whether a requesting device communicating through the interface can access a service it has requested access to, arranged to store trust indications in association with requesting devices and arranged to receive from the interface an indication, originating from the other device, identifying the other device wherein if the requesting device has a stored trust indication associated therewith, no user authorization is required, and if the requesting device has no stored trust indication associated therewith, user authorization being required.

The examiner alleges that Orita discloses two authentications--that the first authentication (input of the user ID and password) is "a standard login that is well known in the art of networking" and that the second authentication is the input of "EP authenticating parameters in order to access the secure resources". The examiner considers that the first authentication is separate to the second authentication. Consequently, the examiner makes the conclusion that "the user can access a system first without having to prove that he\she has access to any particular network resources" and that "it is only when the user requests the resources must he\she

provide the EP [password]".

Orita discloses that a user ID and password, input by a user into the work station 10, are searched against OP information, stored on a storage unit 12c. If they match one another, the user is recognized as a registered user and is allowed to log on to the system. At this stage, OP information is read out from the storage unit 12c and stored in area 14a of the host computer 11. One user program is stored in one EP information file and a user who is entitled to access the EP information file can open the user program stored in the EP information file. An EP password is entered by the user, along with the name of the EP information file, in order to check whether access to an EP information file is allowed or prohibited (see col. 3 lines 63 - 67). The EP password can be shared amongst many users (Col. 5, lines 56-59). Additionally, access to the EP information file is determined by an EP authority level which is compared with the authority level of the operator profile (see col. 3 line 67 to col. 4, line 8). The EP authority level appears to be an authority level that is associated with the EP information file, which can be shared amongst many users. The EP authority level is not associated with the identity of the user. If the check is successful, the host computer 11 reads the EP information 12d, defined by the OP information 12c, out of the storage unit 12 and stores it in the host computer 11.

If a user has access to the EP information file on the host computer 11, he may activate a user program defined in the EP information file to access and modify files. In order to access a file, the user program checks whether a password stored in the EP information file corresponds to a password contained in access protection information 12a of the file to be accessed (see col. 4, line 52 to col. 5 line 37). The access protection information includes information on the password and access type

of a file and is contained within the file. In addition, the user program is allotted with an authority level, and access to the file by the user is prohibited if the user's authority level (as defined by the OP information) is lower than that of the user program. When a request to access a file is permitted, determination of permission of execution of access is made based on the access protection information (see col. 5, lines 30 to 34).

Therefore, Orita merely discloses that a file contains access protection information including a password and type of access. Access to a file depends on a password contained in the EP information file and the authority level of the user contained in the OP. Access to a program depends on the input EP password and the authority level of the user contained in the OP. Consequently, neither access to a file or a program requires user authentication at the point of access but does require user authentication at logon to obtain the OP. It is therefore essential that user authentication and obtaining OP information occurs before determining whether access to a file / program should be allowed.

The examiner is incorrect in his assessment of Orita. The examiner alleges that the input of user ID is independent of the input of an EP password to access user programs or files. As described on col. 3, line 53 to col. 4, line 9, the operator profile authority level is used in combination with the EP password to determine whether access to an EP information file is allowed and hence access to a user program. The operator profile is previously downloaded from the storage unit 14 to the host computer 11 in response to the input of a user ID and password that corresponds to an operator profile. Therefore, the Examiner has misinterpreted Orita. Orita discloses that access to an EP information file is dependent upon the OP authority level which is provided by the authentication of the user. Moreover, as mentioned above,

determination of access to a file is also made by comparing the authority level of the user (as defined by the operator profile) with the authority level of the program. Thus, access to a file is dependent upon the OP authority level.

Therefore, Orita does not disclose or suggest access control means accessible by a communicating device requesting access to the first application without the communicating device having been authenticated by the authentication means, as recited in the claims of the present application. In Orita, a user must always input their user ID and password and be authenticated by the computer system in order to obtain an OP and then access user programs or files.

Additionally, Orita teaches that the EP information may not be specific to an individual user, but generic to a group of users. In this case, the EP information would be incapable of identifying and authenticating a specific user. Therefore, even if we view Orita in line with the examiners assertion that the entering of an EP password is a separate authentication, the resultant computer system would not be able to authenticate a specific user. Consequently, the teaching of Orita is clear, the purpose of the input of the user ID and password is to first authenticate a user. The EP information, in combination with the OP information, is used to provide a level of security for user programs and files once the user has been authenticated.

The Examiner reasserts that Orita discloses access control means accessible by a communicating device requesting access to a first application without the communicating device having been authenticated by the authenticating means, . . . as recited in the claims of the present application, in Orita at col. 1, lines 51-56 and col. 2, lines 10-19. However, as noted in Applicants' previously-filed response, these portions of Orita merely disclose a computer system having a security function

capable of attaining the security according to the content of a file and the access type at the time of accessing file by a user so as to affect a reliable security operation for files, and that it is determined whether execution of file access is permitted or not based on the access protection information read out from a second storage unit when an access request is made with respect to a specified file stored in a first storage unit according to a user program. This is not a communicating device requesting access to a first application without the communicating device having been authenticated by an authentication means, and arranged to arbitrate whether access of the communicating device to the first application is granted or refused wherein if the arbitration requires an authentication of the communicating device, the access control means instructing the authentication means to authenticate the communicating device, as recited in the claims of the present application. These portions of Orita do not disclose or suggest a communicating device requesting access to an application, or determining whether a communicating device has been authenticated by an authentication means. Further, these portions of Orita do not disclose or suggest an authentication means to authenticate a communicating device if arbitration requires an authentication of the communicating device. These portions of Orita merely disclose attaining security according to the content of a file where execution of file access is determined based on the access protection information read out from a storage unit. The claims of the present application relate to access to an application. In contrast, Orita relates to access to a file.

Regarding claims 2-11, 13, 18 and 29, these features to the extent that they have been recited with respect to claims 1 and 28, are not taught or suggested by Orita.

With respect to claim 2, which depends from claim 1, it recites the additional feature of where the access control means is arranged to store security indications in association with accessible applications, wherein the stored security indication associated with the first application is indicative of whether authentication of the communicating device is or is not required during arbitration. Appellants assert that these features are not taught or suggested by Orita.

With respect to claim 3, which depends from claim 1, it recites the additional feature of a user interface for authorizing access to an application during arbitration, the access control means being arranged to store security indications in association with accessible applications, wherein the stored security indication associated with the first application is indicative of whether user authorization of the communicating device is or is not required during arbitration. Appellants assert that these features are not taught or suggested by Orita.

With respect to claim 4, which depends from claim 2, it recites the additional feature of where the stored security indication associated with the first application is indicative of whether authentication of the communicating device is or is not required during arbitration, in independence of the identity of the communicating device. Appellants assert that these features are not taught or suggested by Orita.

With respect to claim 5, which depends from claim 3, it recites the additional feature of wherein the access control means is further arranged to store trust indications in association with devices, and wherein the stored security indication associated with the first application is indicative of whether user authorization of the communicating device is or is not required during arbitration in dependence upon any stored trust indication associated with the communicating device. Appellants assert

that these features are not taught or suggested by Orita.

With respect to claim 6, which depends from claim 1, it recites the additional feature of a user interface for authorizing access to an application during arbitration, the access control means being arranged to store trust indications in association with devices, wherein if there is a stored trust indication associated with the communicating device then no user authorization is required. Appellants assert that these features are not taught or suggested by Orita.

With respect to claim 7, which depends from claim 6, it recites the additional feature of where the access control means receives indications originating from communicating device identifying the communicating device. Appellants assert that these features are not taught or suggested by Orita.

With respect to claim 8, which depends from claim 1, it recites the additional feature of a user interface for authorizing access to an application during arbitration, the access control means being arranged to store trust indications in association with devices and to store security indications in association with accessible applications, wherein if there is a stored trust indication associated with the communicating device then no user authorization is required and if there is no trust indication associated with the communing device user authorization is required in dependence on the stored security indication associated with the requested application. Appellants assert that these features are not taught or suggested by Orita.

With respect to claim 9, which depends from claim 5, it recites the additional feature of where the access control means receives indications originating from the communicating device identifying the communicating device and the application requested. Appellants assert that these features are not taught or suggested by Orita.

With respect to claim 10, which depends from claim 1, it recites the additional feature of having a device database which stores trust indications of different devices. Appellants assert that these features are not taught or suggested by Orita.

With respect to claim 11, which depends from claim 1, it recites the additional feature of having a service database for storing security indications of the accessible applications. Appellants assert that these features are not taught or suggested by Orita.

With respect to claim 13, which depends from claim 1, it recites the additional feature of where the access control means is an/the interface with the first application. Appellants assert that these features are not taught or suggested by Orita.

With respect to claim 18, which depends from claim 1, it recites the additional feature of a plurality of applications and a plurality of access control means where each application has an access control means connected to it. Appellants assert that these features are not taught or suggested by Orita.

With respect to claim 29, which depends from claim 28, it recites the additional feature of where the determination is made on the basis of the identity of service requested and/or the identity of the requesting device. Appellants assert that these features are not taught or suggested by Orita.

Appellants assert that the Orita reference cited by the Examiner in the Office Action does not disclose or suggest the limitations in the claims of the present application. Moreover, the Examiner has failed to meet the required legal burden as set forth by the courts and the M.P.E.P. to substantiate valid rejections under 35 U.S.C. 102(b). Accordingly, the Examiner has failed to make a proper prima facie case of anticipation for the Orita rejections. Appellants respectfully request that these

rejections be withdrawn, the decision of the Examiner be reversed, and that these claims be allowed.

Rejections have also been based on a combination of references being asserted by the Examiner under 35 U.S.C. §103(a). The ultimate determination of obviousness under §103 is a question of law. *See*, *In re Leuders*, 111 F.3d 1569, 1571, 42USPQ2d 1481, 1482 (Fed. Cir. 1997). The factual predicates underlying an obviousness determination include the scope and content of the prior art, the differences between the prior art and the claimed invention, and the level of ordinary skill in the art at the time of the invention. *See*, *Monarch Knitting Mach. Corp. v. Sulzer Morat GmbH*, 139 F.3d 877, 881, 45 USPQ2d 1977, 1981 (Fed. Cir. 1998).

To reject claims in an application under Section 103, an Examiner must show an unrebutted prima facie case of obviousness. *See*, *In re Deuel*, 51 F.3d 1552, 1557, 34 USPQ2d 1210, 1214 (Fed. Cir. 1995). In the absence of a proper prima facie case of obviousness, an applicant who complies with the other statutory requirements is entitled to a patent. *See*, *In re Oetiker*, 977 F.2d 1443, 1445, 24 USPQ2d 1443, 1444 (Fed. Cir. 1992). It is respectfully submitted that the Patent Office has not met the required legal burden as set forth by the courts to substantiate valid rejections under 35 U.S.C. 103(a).

Appellants assert that the references cited by the Examiner in the Office Actions dated December 31, 2003 and May 17, 2004 do not disclose or suggest the limitations in the claims of the present application. Moreover, the Examiner has failed to show a proper motivation to combine the cited references and, therefore, the Patent Office has not made a proper prima facie case of obviousness for any of the rejections.

Claim 12 and Orita in view of Leveridge et al.

Claim 12 stands rejected under 35 U.S.C. §103(a) as being unpatentable over Orita in view of Leveridge et al. Appellants respectfully request that this rejection be reversed.

Leveridge et al. discloses an authentication server being provided which stores authentication details of authorized users, and a list of currently authenticated users. A number of application servers are connected to the authentication server, to allow the authentication servers to check the current authentication status of a user that requires service by the application servers. A session key is generated during the authentication procedure, for use during subsequent communications.

Appellants submit that claim 12 is dependent on independent claim 1 and, therefore, is patentable at least for the same reasons noted previously regarding this independent claim. Appellants submit that Leveridge et al. does not overcome the substantial defects noted previously regarding Orita. Claim 12 recites the additional feature of authentication comprising secret key exchange between the device and the communicating device. Appellants assert that these features are not taught or suggested by the cited references.

Accordingly, Appellants submit that neither Orita nor Leveridge et al. taken alone or in any proper combination, disclose, suggest or render obvious the limitations in the combination of claim 12 of the present application. Appellants respectfully request that this rejection be withdrawn, the decision of the Examiner be reversed, and that this claim be allowed.

Claims 14-17 and 20-26 and Orita in view of Haartsen et al.

Claims 14-17 and 20-26 stand rejected under 35 U.S.C. §103(a) as being

unpatentable over Orita in view of Haartsen et al. Appellants respectfully request that these rejections be reversed.

Haartsen et al. discloses the vision and goals of the BLUETOOTH program and introduces the radio-based technology that consists of a low cost, low power radio-based cable replacement. This technology provides a basis for portable devices to communicate together in an ad hoc fashion by creating personal area networks which have similar advantages to their office environment counterpart, the local area network (LAN). The vision, goals, and architecture of BLUETOOTH are disclosed.

With respect to claim 14, which depends from claim 1, Appellants submit that Haartsen et al. does not overcome the substantial defects noted previously regarding Orita. Claim 14 recites the additional feature of having a protocol stack comprising a first layer and a second higher layer overlying the first layer, with or without, intermediary layers, wherein the first lower layer is the authentication means and the second higher layer is part of the access control means. Appellants assert that these features are not taught or suggested by the cited references.

With respect to claim 15, which depends from claim 14, Appellants submit that Haartsen et al. does not overcome the substantial defects noted previously regarding Orita. Claim 15 recites the additional feature of where the second layer in combination with a security manager is the access control means. Appellants assert that these features are not taught or suggested by the cited references.

With respect to claim 16, which depends from claim 14, Appellants submit that Haartsen et al. does not overcome the substantial defects noted previously regarding Orita. Claim 16 recites the additional feature of where the first layer is the Link Manager Protocol Layer according to the presently proposed BLUETOOTH

specification v0.9 or its equivalent. Appellants assert that these features are not taught or suggested by the cited references.

With respect to claim 17, which depends from claim 14, Appellants submit that Haartsen et al. does not overcome the substantial defects noted previously regarding Orita. Claim 17 recites the additional feature of where the second layer is not the Link Manager Protocol Layer according to the presently proposed BLUETOOTH specification v0.9 or its equivalent. Appellants assert that these features are not taught or suggested by the cited references.

With respect to claim 20, which depends from claim 14, Appellants submit that Haartsen et al. does not overcome the substantial defects noted previously regarding Orita. Claim 20 recites the additional feature of where each access control means includes one of a plurality of different multiplexing protocol layers. Appellants assert that these features are not taught or suggested by the cited references.

With respect to claim 21, which depends from claim 20, Appellants submit that Haartsen et al. does not overcome the substantial defects noted previously regarding Orita. Claim 21 recites the additional feature of where each access control means is the combination of the one multiplexing protocol layer and a security manager. Appellants assert that these features are not taught or suggested by the cited references.

With respect to claim 22, which depends from claim 20, Appellants submit that Haartsen et al. does not overcome the substantial defects noted previously regarding Orita. Claim 22 recites the additional feature of where the access control means for a particular application is the highest possible multiplexing protocol layer associated with that particular application. Appellants assert that these features are not taught or

suggested by the cited references.

With respect to claim 23, which depends from claim 14, Appellants submit that Haartsen et al. does not overcome the substantial defects noted previously regarding Orita. Claim 23 recites the additional feature of where a request to access the first application proceeds up through the protocol stack to the access control means. Appellants assert that these features are not taught or suggested by the cited references.

With respect to claim 24, which depends from claim 21, Appellants submit that Haartsen et al. does not overcome the substantial defects noted previously regarding Orita. Claim 24 recites the additional feature of where each multiplexing protocol layer, in the route of the request as it proceeds up through the protocol stack, queries the security manager which, if the requested application is not connected to the querying protocol layer, allows access of the request through the querying protocol layer to a higher multiplexing protocol layer, and, if the requested application is connected to the querying protocol layer, performs an arbitration to grant or refuse access of the communicating device to the requested application. Appellants assert that these features are not taught or suggested by the cited references.

With respect to claim 25, which depends from claim 15, Appellants submit that Haartsen et al. does not overcome the substantial defects noted previously regarding Orita. Claim 25 recites the additional feature of where the security manager controls the authentication means. Appellants assert that these features are not taught or suggested by the cited references.

With respect to claim 26, which depends from claim 1, Appellants submit that Haartsen et al. does not overcome the substantial defects noted previously regarding

Orita. Claim 26 recites the additional feature of being portable, having a radio transceiver and a user interface comprising a display and user input means. Appellants assert that these features are not taught or suggested by the cited references.

Accordingly, Appellants submit that neither Orita nor Haartsen et al. taken alone or in any proper combination, disclose, suggest or render obvious the limitations in the combination of each of claims 14-17 and 20-26 of the present application. Appellants respectfully request that these rejections be withdrawn, the decision of the Examiner be reversed, and that these claims be allowed.

Claims 19 and 27 and Orita in view of Mashayekhi

Claims 19 and 27 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Orita in view of Mashayekhi. Appellants respectfully request that these rejections be reversed.

Mashayekhi discloses a distributed authentication service that automates an authentication exchange between a user and an application program of a distributed network system. The distributed authentication service includes an exchange controller coupled to an authentication database containing a group of encrypted application secrets associated with the user. Each application secret is, in turn, associated with a particular program resident in the system.

With respect to claim 19, which depends from claim 18, Appellants submit that Mashayekhi does not overcome the substantial defects noted previously regarding Orita. Claim 19 recites the additional feature of where the plurality of access control means are arranged in a hierarchy, wherein a first access control means at the lowest level in the hierarchy provides access to at least a second access control means and

access to one or both of a third access control means and an application, wherein access to each application is provided via one or more access control means including the first access control means and the application's connected access control means, if different, and wherein any access control means is accessible by a communicating device requesting access to one of its connected applications without the communicating device having been authenticated by the authentication means, and is arranged to arbitrate whether access of the communicating device to the one connected application is granted or refused, the connected access control means instructing the authentication means to authenticate the communicating device if the arbitration requires an authentication of the communicating device. Appellants assert that these features are not taught or suggested by the cited references.

With respect to claim 27, Applicants submit that neither Orita nor Mashayekhi, taken alone or in any proper combination, disclose or suggest the limitations in the combination of this claim of, inter alia, first access control means accessible by a communicating device requesting access to the first application program without the communicating device having been authenticated by the authentication means, and arranged to arbitrate whether access of the communicating device to the first application is granted or refused wherein if the arbitration requires an authentication of the communicating device, the access control means instructs the authentication means to authenticate the communicating device, or second access control means accessible by a communicating device requesting access to the second application without the communicating device having been authenticated by the authentication means, and arranged to arbitrate whether access of the communicating device to the second application is granted or refused wherein if the arbitration requires an

authentication of the communicating device, the access control means instructs the authentication means to authenticate the communicating device, wherein the first access control means is accessible by a communicating device requesting access to the second application without the communicating device having been authenticated by the authentication means, and is arranged to provide the access of the communicating device to the second access control means. As has been noted previously, Orita does not disclose or suggest these limitations in the claims of the present application. The Examiner admits that Orita fails to disclose or suggest a second access control means accessible by a communicating device requesting access to a second application . . . as recited in claim 27 of the present application, but asserts that Mashayekhi teaches these limitations at col. 5, lines 56-60 and col. 6, lines 43-59. However, these portions of Mashayekhi merely disclose that a workstation and server nodes may be configured as a distributed authentication service that automates an authentication exchange between a user interface, and that keychain objects associated with one or more application objects have attributes of at least one application secret and a public/private key pair where the application secret contains data used by a particular program to authenticate a user. Application secrets may be grouped according to access control level for each application program (e.g., requiring administrative rights for modification, allowing user modifications). This is not a second access control means accessible by a communicating device requesting access to a second application without the communicating device having been authenticated and the other associated limitations, as recited in the claims of the present application. These portions of Mashayekhi do not disclose or suggest anything related to arbitrating whether access of a communicating device is granted

or refused or if arbitration requires authentication of a communicating device. Further, these portions of Mashayekhi do not disclose or suggest anything related to a first access control means being accessible by a communicating device requesting access to a second application without the communicating device having been authenticated by an authentication means, and arranged to provide the access of the communicating device to the second access means, as recited in the claims of the present application. As noted, Mashayekhi discloses keychain objects associated with one or more application objects have attributes of at least one application secret and a public/private key pair where the application secret contains data used by a particular program to authenticate a user. The claims of the present application relate to authentication of a communicating device. In addition, Applicants do not interpret these portions of Mashayekhi the way the Examiner interprets it to indicate that once a user has been authenticated to system, the user can be authenticated to all of the other applications.

Accordingly, Appellants submit that neither Orita nor Mashayekhi taken alone or in any proper combination, disclose, suggest or render obvious the limitations in the combination of each of claims 19 and 27 of the present application. Appellants respectfully request that these rejections be withdrawn, the decision of the Examiner be reversed, and that these claims be allowed.

Appellants assert that the references cited by the Examiner in the Office Action does not disclose, suggest or render obvious the limitations in the claims of the present application. Moreover, the Examiner has failed to meet the required legal burden as set forth by the courts and the M.P.E.P. to substantiate valid rejections under 35 U.S.C. 103(a). Accordingly, the Examiner has failed to make a proper prima

facie case of obviousness for the cited rejections. Appellants respectfully request that these rejections be withdrawn, the decision of the Examiner be reversed, and that these claims be allowed.

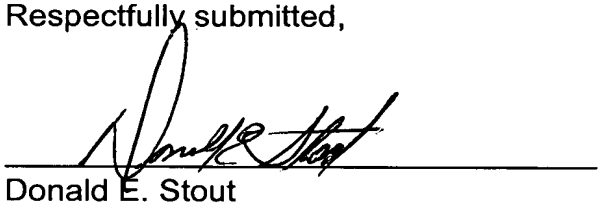
SUMMARY

Appellants submit that the Examiner's rejections of claims1-32 under 35 U.S.C. §102 and 35 U.S.C. §103 are not properly founded in law, and respectfully requests the Board to reverse the Examiner's rejections.

Appellants hereby request an Oral Hearing.

To the extent necessary, applicants petition for an extension of time under 37 C.F.R. section 1.136. Please charge any shortage in the fees due in connection with the filing of this paper, including extension of time fees, to Deposit Account No. 01-2135 (Case No. 1156.41275X00) and please credit any excess fees to such Deposit Account.

Respectfully submitted,



(703) 312-6600
FDB:DES/sdb:dlh

Donald E. Stout
Registration No. 26,422
ANTONELLI, TERRY, STOUT & KRAUS, LLP

APPENDIX

CLAIMS

1. (original) A device for communicating with other devices to allow them to access applications, comprising:

at least a first application;

authentication means for authenticating a communicating device;

access control means accessible by a communicating device requesting access to the first application without the communicating device having been authenticated by the authentication means, and arranged to arbitrate whether access of the communicating device to the first application is granted or refused wherein if the arbitration requires an authentication of the communicating device, the access control means instructs the authentication means to authenticate the communicating device.

2. (original) A device as claimed in claim 1 wherein the access control means is arranged to store security indications in association with accessible applications, wherein the stored security indication associated with the first application is indicative of whether authentication of the communicating device is or is not required during arbitration.

3. (previously presented) A device as claimed in claim 1 further comprising a user interface for authorizing access to an application during arbitration, the access control means being arranged to store security indications in association with accessible applications, wherein the stored security indication associated with the first application is indicative of whether user authorization of the communicating device is or is not required during arbitration.

4. (original) A device as claimed in claim 2 wherein the stored security indication associated with the first application is indicative of whether authentication of the communicating device is or is not required during arbitration, in independence of the identity of the communicating device.

5. (previously presented) A device as claimed in claim 3 wherein the access control means is further arranged to store trust indications in association with devices, and wherein the stored security indication associated with the first application is indicative of whether user authorization of the communicating device is or is not required during arbitration in dependence upon any stored trust indication associated with the communicating device.

6. (previously presented) A device as claimed in claim 1 further comprising a user interface for authorizing access to an application during arbitration, the access control means being arranged to store trust indications in association with devices, wherein if there is a stored trust indication associated with the communicating device then no user authorization is required.

7. (original) A device as claimed in claim 6 wherein the access control means receives indications originating from communicating device identifying the communicating device.

8. (previously presented) A device as claimed in claim 1 further comprising a user interface for authorizing access to an application during arbitration, the access control means being arranged to store trust indications in association with devices and to store security indications in association with accessible applications, wherein if there is a stored trust indication associated with the communicating device then no user authorization is required and if there is no trust indication associated with the communing device user authorization is required in dependence on the stored security indication associated with the requested application.

9. (original) A device as claimed in claim 5 wherein the access control means receives indications originating from the communicating device identifying the communicating device and the application requested.

10. (original) A device as claimed in claim 1 having a device database which stores trust indications of different devices.

11. (original) A device as claimed in claim 1 having a service database for storing security indications of the accessible applications.

12. (original) A device as claimed in claim 1 wherein authentication comprises secret key exchange between the device and the communicating device.

13. (original) A device as claimed in claim 1 wherein the access control means is an/the interface with the first application.

14. (original) A device as claimed in claim 1 having a protocol stack comprising a first layer and a second higher layer overlying the first layer, with or without, intermediary layers, wherein the first lower layer is the authentication means and the second higher layer is part of the access control means.

15. (original) A device as claimed in claim 14 wherein the second layer in combination with a security manager is the access control means.

16. (previously presented) A device as claimed in claim 14 wherein the first layer is the Link Manager Protocol Layer according to the presently proposed BLUETOOTH specification v0.9 or its equivalent.

17. (previously presented) A device as claimed in claim 14 wherein the second layer is not the Link Manager Protocol Layer according to the presently proposed BLUETOOTH specification v0.9 or its equivalent.

18. (original) A device as claimed in claim 1 comprising a plurality of applications and a plurality of access control means where each application has an access control means connected to it.

19. (original) A device as claimed in claim 18 wherein the plurality of access control means are arranged in a hierarchy, wherein a first access control means at the lowest level in the hierarchy provides access to at least a second access control

means and access to one or both of a third access control means and an application, wherein access to each application is provided via one or more access control means including the first access control means and the application's connected access control means, if different, and wherein any access control means is accessible by a communicating device requesting access to one of its connected applications without the communicating device having been authenticated by the authentication means, and is arranged to arbitrate whether access of the communicating device to the one connected application is granted or refused, the connected access control means instructing the authentication means to authenticate the communicating device if the arbitration requires an authentication of the communicating device.

20. (previously presented) A device as claimed in claim 14 wherein the or each access control means includes one of a plurality of different multiplexing protocol layers.

21. (previously presented) A device as claimed in claim 20 wherein each access control means is the combination of the one multiplexing protocol layer and a security manager.

22. (original) A device as claimed in claim 20 or wherein the access control means for a particular application is the highest possible multiplexing protocol layer associated with that particular application.

23. (original) A device as claimed in claim 14 wherein a request to access the first application proceeds up through the protocol stack to the access control means.

24. (original) A device as claimed in claim 21 wherein each multiplexing protocol layer, in the route of the request as it proceeds up through the protocol stack, queries the security manager which, if the requested application is not connected to the querying protocol layer, allows access of the request through the querying protocol layer to a higher multiplexing protocol layer, and, if the requested application is connected to the querying protocol layer, performs an arbitration to grant or refuse access of the communicating device to the requested application.

25. (original) A device as claimed in claim 15 wherein the security manager controls the authentication means.

26. (original) A device as claimed in claim 1 being portable, having a radio transceiver and a user interface comprising a display and user input means.

27. (previously presented) A device for communicating with other devices to allow them to access applications, comprising:

at least first and second applications;

authentication means for authenticating a communicating device;

first access control means accessible by a communicating device requesting access to the first application without the communicating device having been authenticated by the authentication means, and arranged to arbitrate whether access

of the communicating device to the first application is granted or refused wherein if the arbitration requires an authentication of the communicating device, the first access control means instructs the authentication means to authenticate the communicating device;

second access control means accessible by a communicating device requesting access to the second application without the communicating device having been authenticated by the authentication means, and arranged to arbitrate whether access of the communicating device to the second application is granted or refused wherein if the arbitration requires an authentication of the communicating device, the second access control means instructs the authentication means to authenticate the communicating device, wherein the first access control means is accessible by a communicating device requesting access to the second application without the communicating device having been authenticated by the authentication means, and is arranged to provide the access of the communicating device to the second access control means.

28. (original) A method of arbitrating the access of a requesting device to a service provided by a providing device comprising:

sending a request to access the service from the requesting device to the providing device;

receiving the request at the providing device and passing it, without authenticating the requesting device, to an arbitration means interfacing the service;

determining, in the arbitration means, whether to grant or refuse access to the first application by the requesting device, wherein if the determination requires an

authentication of the requesting device, the authentication is performed during that determination and not previously.

29. (original) A method as claimed in claim 28 wherein the determination is made on the basis of the identity of service requested and/or the identity of the requesting device.

30. (previously presented) A device for providing services and allowing access by other devices to the provided services, comprising:

an interface for communicating with the other devices and receiving requests to access a service therefrom;

arbitration means, for determining whether a requesting device communicating through the interface can access a service it has requested access to, arranged to store trust indications in association with requesting devices and arranged to receive from the interface an indication, originating from the other device, identifying the other device, wherein, if the requesting device has a stored trust indication associated therewith no user authorization is required and if the requesting device has no stored trust indication associated therewith user authorization is requirable; and

a user interface for providing user authorization.

31. (previously presented) A device for providing services and allowing access by other devices to the provided services, comprising:

an interface for communicating with the other devices and receiving requests to access a service therefrom;

arbitration means, for determining whether a requesting device communicating through the interface can access a service it has requested access to, arranged to store trust indications in association with requesting devices and store security indications in association with provided services and arranged to receive from the interface indications, originating from the other device, identifying the other device and the service requested, wherein, if the requesting device has a stored trust indication associated therewith no user authorization is required and if the requesting device has no stored trust indication associated therewith user authorization is required in dependence upon the stored security indication associated with the requested service;

and a user interface for providing user authorization.

32. (previously presented) A device for communicating with other devices to allow them to access applications, comprising:

at least a first application;

authentication means for authenticating a communicating device;

access control means accessible by a communicating device requesting access to the first application without the communication device having been authenticated by the authentication means, and arranged to arbitrate whether access of the communicating device to the first application is granted or refused, wherein arbitration is dependent upon the identity of the first application and if the arbitration requires an authentication of the communicating device, the access control means instructs the authentication means to authenticate the communicating device.